Vol 14 No 3, March 2005
1009-1963/2005/14(03)/0541-05

Chinese Physics

A quantum identification scheme based on polarization modulation*

He Guang-Qiang(何广强)† and Zeng Gui-Hua(曾贵华)

The State Key Laboratory on Fibre-Optic Local Area Networks and Advanced Optical Communication Systems, Electronic Engineering Department, Shanghai Jiaotong University, Shanghai 200030, *China*

(Received 21 June 2004; revised manuscript received 27 July 2004)

A quantum identification scheme including registration and identification phases is proposed. The users' passwords are transmitted by qubit string and recorded as a set of quantum operators. The security of the proposed scheme is guaranteed by the no-cloning theorem. Based on photon polarization modulation, an experimental approach is also designed to implement our proposed scheme.

Keywords: quantum identification, quantum cryptography, cryptography
PACC: 4250, 4230Q, 0365

1. Introduction

Quantum cryptography is a field combining quantum and information theories. Since the first quantum key distribution protocol–BB84 protocol was presented by Bennett and Brassard,[1] many advanced topics in quantum cryptography have been put forward including, in recent years, enhanced insight into the basic theory,[2] quantum key management,[3] quantum key sharing,[4] quantum authentication,[5] quantum-bit commitment[6] and quantum random number generator.[7,8] In contrast to the classical cryptography, which is only relatively secure, quantum cryptography exhibits absolute security due to its intrinsic quantum characteristics. In particular, quantum key distribution (QKD) attracts much attention from both academic and commercial sectors because of its unconditional security and greater possibility of implementation.

Experiments on quantum key distribution may be implemented through two quantum channels: free space[9] and optic fibre.[10] Kurtsiefer *et al*[11] at Ludwig–Maximilians–University reported on a BB84-based free space quantum cryptography system over 23.4km in 2002. The research group lead by Professor N Gisin of Geneva University designed an auto-compensating plug & play system[12] over the installed optic fibre in 2002, and the keys were exchanged over a distance of 67km. Very few papers on quantum identification system have been published. Utilizing BB84-based quantum key distribution in conjunction with classical identification, Miloslav Dusek *et al* reported a quantum identification scheme,[13] in which Alice and Bob verify each other's identity by three handshakes. Unfortunately, this scheme was later proved to be a classical identification scheme. In this paper, a quantum identification scheme to dynamically build the users' database according to the password and the identity card of the legitimate user is presented. The security of the scheme is guaranteed by the no-cloning theorem of the unknown quantum state.

In Section 2, we investigate the general principle required for a quantum identification scheme. The new quantum identification scheme is introduced in detail in Section 3. The proposed scheme includes a registration phase and an identification phase. In Section 4, we discuss the security of the proposed scheme. In Section 5, the experimental system based on photon polarization modulation is proposed for carrying out this quantum identification scheme. Conclusions are drawn in Section 6.

2. General requirement

Classical cryptography protocols and algorithms

*Project supported by the Natural Science Foundation of China (Grant Nos 60102001 and 90104005).
†E-mail: gqhe@sjtu.edu.cn

based on the mathematical problems are designed in the fields of both cryptography and secure communication. Similarly, quantum cryptography protocols and algorithms based on the basic theories and the phenomena of quantum physics are proposed in the same fields. Several aspects such as key distribution, secret sharing and digital signature, which have been studied in classical cryptography, are still investigated in quantum cryptography. The difference is that quantum cryptography relies on quantum physics. The theoretical basis of our quantum identification scheme is the no-cloning theorem of unknown quantum state that reads as follows.

No-cloning theorem: An unknown quantum state cannot be absolutely copied.

Cloning a quantum state means to produce the same quantum state in another quantum system, at the same time, while not changing the initial quantum state. The no-cloning theorem is a direct result of quantum mechanics. It is the foundation of quantum cryptography and also prevents the quantum computer from copying the unknown quantum state.

3. Description of the proposed quantum identification scheme

In the proposed scheme, U^k denotes the kth user, IS is the identification system. Suppose that quantum channel is an unjammable channel; in addition, the illegitimate users in general cannot enter into the identification system.

The proposed scheme includes a registry phase and an identification phase. During the registry phase, the identification system dynamically builds the users' information in the users' database after it receives the uses' registry requests. In the identification phase, the identification system verifies the user's identity according to the corresponding user's information in the users' database.

The proposed scheme (Fig.1.) is described in the following.

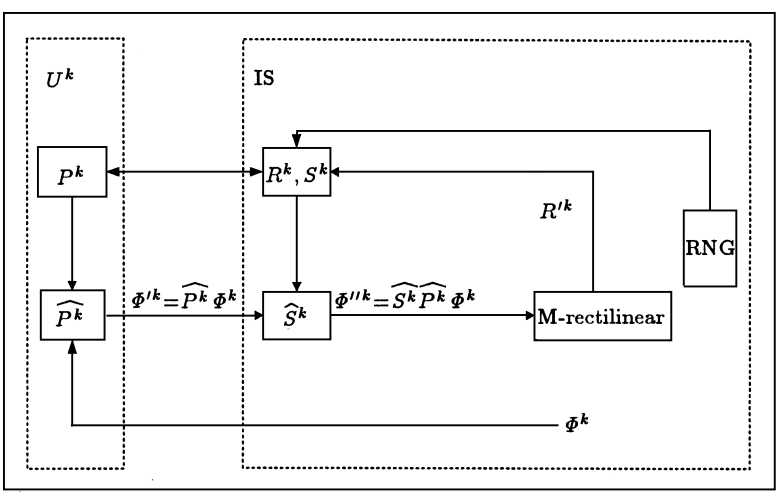

Fig.1. Quantum identification scheme.

3.1. Registration phase

(1) When the identification system (IS) receives the registry requirement of the user U^k, it prepares a set of initial quantum states, $\Phi^k = (|\phi_1^k\rangle, |\phi_2^k\rangle, \cdots, |\phi_n^k\rangle)$ taking the form $|\phi_i^k\rangle = |0\rangle$, $i \in \{1, 2, \cdots, n\}$. The user U^k sets up the password $P^k = (p_1^k, p_2^k, \cdots, p_n^k)$, $p_i^k \in \{1, 2, \cdots, m\}$, $i \in \{1, 2, \cdots, n\}$, P^k corresponds to a set of quantum operations, which are denoted by a set of quantum operators $\widehat{P^k} = (\widehat{p_1^k}, \widehat{p_2^k}, \cdots, \widehat{p_n^k})$. Note that the number p_i^k corresponds to the special quantum operator $\widehat{p_i^k}$. If $p_i^k \neq p_j^k$, then $\widehat{p_i^k} \neq \widehat{p_j^k}$. The password P^k is transmitted to IS by quantum key distribution (for example BB84 protocol[1]) or secure channel. Then IS knows the corresponding quantum operator $\widehat{P^k} = (\widehat{p_1^k}, \widehat{p_2^k}, \cdots, \widehat{p_n^k})$. Both IS and U don't know the key during quantum key distribution, they gain the key after finishing quantum key distribution.[1]

(2) IS prepares an n-bit random number $R^k = (r_1^k, r_2^k, \cdots, r_n^k)$, $r_i^k \in \{0, 1\}$, $i \in \{1, 2, \cdots, n\}$, for the user U^k at the same time, and sets up the information of the user U^k,$S^k = (s_1^k, s_2^k, \cdots, s_n^k)$, $s_i^k \in$

$\{1,2,\cdots,m\}$, $i \in \{1,2,\cdots,n\}$ in the users' database. S^k corresponds to a set of quantum operations, which are denoted by a set of quantum functors $\widehat{S^k} = (\widehat{s_1^k}, \widehat{s_2^k}, \cdots, \widehat{s_n^k})$, subjected to the following conditions: For $1 \le i \le n$,

if $r_i^k = 0$, then $|\phi_i^{''k}\rangle = \widehat{s_i^k}\widehat{p_i^k}|\widehat{\phi_i^k}\rangle = |0\rangle$, that is to say, $\widehat{s_i^k}\widehat{p_i^k} = I$,

if $r_i^k = 1$, then $|\phi_i''^k\rangle = \widehat{s_i^k}\widehat{p_i^k}|\phi_i^k\rangle = |1\rangle$, that is to say, $\widehat{s_i^k}\widehat{p_i^k} = \widehat{\sigma_x}$

Now the messages $R^k = (r_1^k, r_2^k, \cdots, r_n^k)$, $r_i^k \in \{0,1\}$, $i \in \{1,2,\cdots,n\}$ and $S^k = (s_1^k, s_2^k, \cdots, s_n^k)$, $s_i^k \in \{1,2,\cdots,m\}$, $i \in \{1,2,\cdots,n\}$ are used as the information of the user U^k in the users' database. When the user U^k sets up the certainly password $P^k = (p_1^k, p_2^k, \cdots, p_n^k)$, $p_i^k \in \{1,2,\cdots,m\}$, $i \in \{1,2,\cdots,n\}$, then $R^k = (r_1^k, r_2^k, \cdots, r_n^k)$, $r_i^k \in \{0,1\}$, $i \in \{1,2,\cdots,n\}$ has the certainly corresponding relation with $S^k = (s_1^k, s_2^k, \cdots, s_n^k)$, $s_i^k \in \{1,2,\cdots,m\}$. The fact must be emphasized.

After the user completes the registry phase, the password of the user U^k is $P^k = (p_1^k, p_2^k, \cdots, p_n^k)$, $p_i^k \in \{1,2,\cdots,m\}$, $i \in \{1,2,\cdots,n\}$, the file named as U^k in the users' database contains the user U^k's identity messages

$$R^k = (r_1^k, r_2^k, \cdots, r_n^k), \quad r_i^k \in \{0,1\},$$

$$i \in \{1,2,\cdots,n\}$$

and

$$S^k = (s_1^k, s_2^k, \cdots, s_n^k), \quad s_i^k \in \{1,2,\cdots,m\},$$

$$i \in \{1,2,\cdots,n\}.$$

Repeat the steps (1) and (2); many users can register the quantum identification system.

3.2. Identification phase

(3) IS finds the file U^k from the users' database according to the file name U^k when it receives the identification requirement of the user U^k. The registry messages $R^k = (r_1^k, r_2^k, \cdots, r_n^k)$, $r_i^k \in \{0,1\}$, $i \in \{1,2,\cdots,n\}$ and $S^k = (s_1^k, s_2^k, \cdots, s_n^k)$, $s_i^k \in \{1,2,\cdots,m\}$, $i \in \{1,2,\cdots,n\}$ are used to identify the user U^k.

(4) The user U^k inputs the password $P^k = (p_1^k, p_2^k, \cdots, p_n^k)$, $p_i^k \in \{1,2,\cdots,m\}$, $i \in \{1,2,\cdots,n\}$, IS applies a set of corresponding quantum operators $\widehat{P^k} = (\widehat{p_1^k}, \widehat{p_2^k}, \cdots, \widehat{p_n^k})$ to a set of initial quantum states $\Phi^k = (|\phi_1^k\rangle, |\phi_2^k\rangle, \cdots, |\phi_n^k\rangle)$, $|\phi_i^k\rangle = |0\rangle$, $i \in \{1,2,\cdots,n\}$, and obtains a set of quantum states $\Phi'^k = (|\phi_1'^k\rangle, |\phi_2'^k\rangle, \cdots, |\phi_n'^k\rangle)$, $|\phi_i'^k\rangle = \widehat{p_i^k}|\phi_i^k\rangle$, $i \in \{1,2,\cdots,n\}$.

(5) IS verifies whether the information $S^k = (s_1^k, s_2^k, \cdots, s_n^k)$, $s_i^k \in \{1,2,\cdots,m\}$, $i \in \{1,2,\cdots,n\}$ is right or not. IS applies a set of corresponding quantum operators $\hat{S}^k = (s_1^k, s_2^k, \cdots, s_n^k)$ to a set of initial quantum states $\Phi'^k = (|\phi_1'^k\rangle, |\phi_2'^k\rangle, \cdots, |\phi_n'^k\rangle)$, $|\phi_i'^k\rangle = \widehat{p_i^k}|\phi_i^k\rangle$, $i \in \{1,2,\cdots,n\}$ and obtains a set of quantum states $\Phi''^k = (|\phi_1''^k\rangle, |\phi_2''^k\rangle, \cdots, |\phi_n''^k\rangle)$, $|\phi_i''^k\rangle = \widehat{s_i^k}\widehat{p_i^k}|\phi_i^k\rangle$, $i \in \{1,2,\cdots,n\}$.

(6) IS measures a set of quantum states $\Phi''^k = (|\phi_1''^k\rangle, |\phi_2''^k\rangle, \cdots, |\phi_n''^k\rangle)$, $|\phi_i''^k\rangle = \widehat{s_i^k}\widehat{p_i^k}|\phi_i^k\rangle$, $i \in \{1,2,\cdots,n\}$ adopting rectilinear base, and obtains a set of quantum states

$$R'^k = (|r_1'^k\rangle, |r_2'^k\rangle, \cdots, |r_n'^k\rangle), \quad r_i'^k \in \{0,1\}.$$

According to the following rule: $0 \leftrightarrow |0\rangle$, $1 \leftrightarrow |1\rangle$, we can obtain the n-bit random number

$$R'^k = (r_1'^k, r_2'^k, \cdots, r_n'^k), \quad r_i'^k \in \{0,1\}.$$

(7) Compare $R'^k = (r_1'^k, r_2'^k, \cdots, r_n'^k)$, $r_i'^k \in \{0,1\}$ with $R^k = (r_1^k, r_2^k, \cdots, r_n^k)$, $r_i^k \in \{0,1\}$. For $1 \le i \le n$, if $r_i'^k = r_i^k$, $i \in \{1,2,\cdots,n\}$, then the identification is successful; otherwise it fails.

4. Security analyses

We take the quantum and classical attacks into account to analyse the security of the quantum identification scheme.

Quantum attack: clone the string of quantum bits Φ'. The attacker needs a specially designed quantum machine which can clone the string of quantum bits Φ'. Quantum bits transmitted by the quantum channel are unknown to eavesdropper, so no-cloning theorem prevents eavesdropper from copying the string of quantum states Φ'.

Classical attack: guess the user's password $P^k = (p_1^k, p_2^k, \cdots, p_n^k)$, $p_i^k \in \{1,2,\cdots,m\}$, $i \in \{1,2,\cdots,n\}$, that is to say, forecast the quantum manipulations $\widehat{P^k} = (\widehat{p_1^k}, \widehat{p_2^k}, \cdots, \widehat{p_n^k})$. If $\widehat{p_i^k}$ is one of the m quantum manipulations, then the probability that the eavesdropper guesses the user's password correctly is $1/m^n$ which will be 0 if IS increases m, n.

To sum up, the proposed scheme can efficiently prevent eavesdropping and cheating, and is absolutely secure to quantum attack.

5. Quantum identification system based on polarization modulation

The quantum identification system based on polarization modulation consists of the identification server terminal (IS) and the user terminal (U) (Fig.2). IS includes an optical path unit and a control unit. The optical path unit includes the diode laser (laser), optical attenuator (Att), polarizer 1 (P_1), dynamic polarization controller 2 (DPC2), polarizer 2 (P_2) and single photon detector (D). The control unit includes main controller 2, users' database and random number generator. U also consists of an optical path unit and a control unit. The optical path unit includes reflection mirrors M_1, M_2, user identity card (UIC), and dynamical polarization controller 1 (DPC1). The control unit includes main controller 1 and synchronous clock generator. The quantum signal generator consisting of the diode laser and optical attenuator generates quasi-single photon carrying quantum information. P_1 initializes the polarization state of the quasi-single photon as the vertical linear polarization state. Then the photon is transmitted to the user terminal in free space. M_1, M_2 change the transmission direction of photons. Both UIC and DPC1 modulate the polarization state of quasi-single photon according to the users' identity card and password. The photon carrying the user identity information is transmitted to IS in free space again. DPC2 modulates the polarization state of the photon according to the users' registry information in the users' database. P_2 determines that the polarization state of photon is vertical linear polarization state or horizontal linear polarization state. D operated in Geiger mode detects the quasi-single photon. It is emphasized that the optical axis of P_1 is parallel to the optical axis of P_2. Controller 1 controls DPC1 according to the user's password. Controller 2 controls DPC2 according to the users' registry information in users' database. Controller 1 communicates with Controller 2 by classical channel. Synchronous clock generator synchronizes Controller 1 with Controller 2. Random number generator produces random number for Controller 2. The users' database stores the users' registry information. The proposed scheme includes a registry phase and an identification phase.

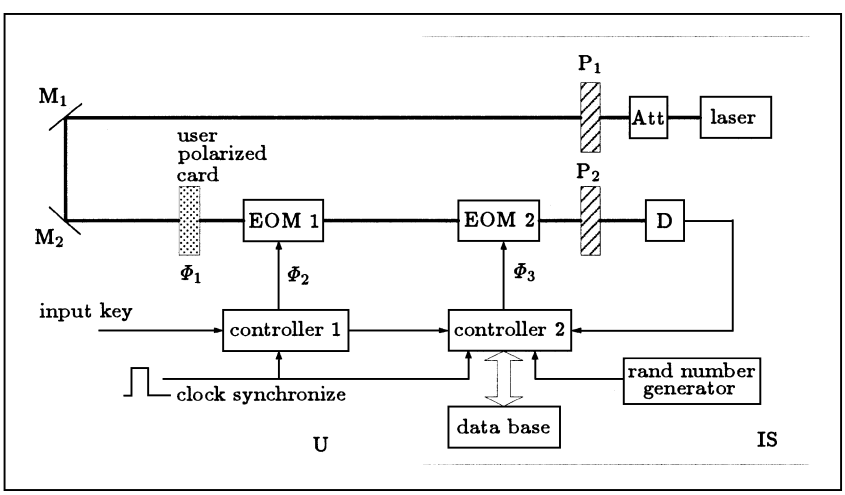

Fig.2. Experimental set-up of quantum identification system laser: diode laser DL-100(780nm); Att: optical attenuator; M_1, M2: reflection mirrors; UIC: user identity card; P_1, P_2: polarizers; DPC1, DPC2: dynamic polarization controllers; Controller 1, Controller 2: main controllers; D: single photon detector.

5.1. Registration phase

(1) User U^k applies for the identity card and sets up the password.

The user plugs in the UIC, a special birefringence crystal capable of rotating the polarization direction of the linear polarization light, and rotates the vertical polarization light. An arbitrary angle Φ_1^k between the polarization plane of incidence light and the polarization plane of the processed linear polarization light is only determined by the UIC. The user U^k sets up the password $P^k = (p_1^k, p_2^k, \cdots, p_n^k)$, $p_i^k \in \{0,1\}$, $i \in \{1,2,\cdots,n\}$, p_i^k drives DPC1 during the ith time slot and rotates the linear polarization light by an angle Φ_{2i}^k again, Φ_{2i}^k corresponds to p_i^k. The password P^k is transmitted to IS by quantum key distribution (for example BB84 protocol[1]) or secure channel. Then IS knows the corresponding angle $\Phi_2^k = (\Phi_{21}^k, \Phi_{22}^k, \cdots, \Phi_{2n}^k)$. Both IS and U don't know the key during quantum key distribution, they gain the key after finishing quantum key distribution.

(2) IS builds the corresponding user's registry in-

formation in the users' database.

Random number generator produces the random number $R^k = (r_1^k, r_2^k, \cdots, r_n^k)$, $r_i^k \in \{0,1\}$, $i \in \{1,2,\cdots,n\}$ needed by IS. IS adjusts DPC2 during the ith time slot and rotates the polarization plate by an angle Φ_{3i}^k subjected to the following conditions:

For $1 \leq i \leq n$,

if $r_i^k = 0$, then $\Phi_1^k + \Phi_{2i}^k + \Phi_{3i}^k = 0^\circ$ or 180°, that is to say, D can detect single photon;

if $r_i^k = 1$, then $\Phi_1^k + \Phi_{2i}^k + \Phi_{3i}^k = 90^\circ$ or 270°, that is to say, D can't detect single photon.

We can obtain a set of random phases $\Phi_3^k = (\Phi_{31}^k, \Phi_{32}^k, \cdots, \Phi_{3n}^k)$ corresponding to $R^k = (r_1^k, r_2^k, \cdots, r_n^k)$.

(3) IS builds the user U^k file in the user database.

File name: U^k

File content: $R^k = (r_1^k, r_2^k, \cdots, r_n^k)$ and $\Phi_3^k = (\Phi_{31}^k, \Phi_{32}^k, \cdots, \Phi_{3n}^k)$

(4) Repeat steps (1)–(3), IS can build many users' registry information in the users' database. The random number must be subjected to the following condition:

If $i \neq j$, then $R^i = (r_1^i, r_2^i, \cdots, r_n^i) \neq R^j = (r_1^j, r_2^j, \cdots, r_n^j)$.

5.2. Identification phase

(5) The user applies for the identification, IS searches the file U^k in the users' database.

If the user U^k wants to enter IS, he tells IS the filename U^k via the classical channel. Then he plugs in his UIC, and inputs his password. IS finds the file U^k according to filename U^k:

$$U^k : R^k = (r_1^k, r_2^k, \cdots, r_n^k)$$

and

$$\Phi_3^k = (\Phi_{31}^k, \Phi_{32}^k, \cdots, \Phi_{3n}^k)$$

(6) IS verifies the user U^k identity information.

The user U^k inputs the password p_i^k during the ith time slot. Both UIC and p_i^k rotate the linear polarization light by an angle $\Phi_1^k + \Phi_{2i}^k$. DPC2 controlled by controller2 rotates the linear polarization light further by an angle Φ_{3i}^k.

(7) IS detects quasi-single photon and verifies the user U^k identity.

Monitoring single photon detector (D), IS gains the classical bit $r_i'^k$ according to the following rule:

If D detects photon, then $r_i'^k = 0$; otherwise $r_i'^k = 1$.

Repeat steps (5)–(7), for $1 \leq i \leq n$, if $r_i'^k = r_i^k$, $i \in \{1,2,\cdots,n\}$, then identification is successful; otherwise the identification fails.

6. Conclusions

A quantum identification scheme based on the manipulation of quantum state is proposed in this paper. This scheme can verify the identity of the legitimate user, and can prevent the eavesdropper from impersonating the legitimate user. The quantum states transmitted by the quantum channel are unknown to the eavesdropper, so this scheme is absolutely secure to quantum attack according to no-cloning theorem. In addition, a quantum identification experimental scheme based on polarization modulation is designed in order to implement the proposed quantum identification scheme.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) pp175–179

[2] Schumacher B 1998 *Phys. Rev. Lett.* **80** 5695

[3] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[4] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[5] Zeng G H and Zhang W P 2000 *Phys. Rev.* A **61** 032303

[6] Kent A 1999 *Phys. Rev. Lett.* **83** 1447

[7] Feng M M *et al* 2003 *Acta Phys. Sin.* **52** 72 (in Chinese)

[8] Liao J *et al* 2001 *Acta Phys. Sin.* **50** 467 (in Chinese)

[9] Betheume D S and Risk W P 2000 *IEEE J. Quantum Electron.* **36** 340

[10] Liang C *et al* 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese)

[11] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P, Tapster P and Rarity J 2002 *Nature* **419** 450

[12] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41.1

[13] Dusek M, Haderka O, Hendrych M and Myska R 1999 *Phys. Rev.* A **60** 149